

REMARKS

Claims 1-19 were pending in the current application. Applicant has canceled claims 1-12, amended claims 13 and 17, and added new claims 20-31. Claims 13-31 are therefore currently pending. Reexamination and reconsideration of all claims, as amended, are respectfully requested.

§ 112

The Office Action rejected claims 18 and 19 under 35 U.S.C. § 112 based on certain preamble wording. Applicants have amended claims 18 and 19 to correct these minor typographical errors and submit that all claims now fully comply with § 112.

§ 103

The Office Action rejected claims 1-19 under 35 U.S.C. § 103(a) based on de la Huerga, U.S. Patent 5,960,085 (“de la Huerga ‘085”) in view of de la Huerga, U.S. Patent 6,346,886 (“de la Huerga ‘886”).

Applicants particularly wish to focus attention on the de la Huerga ‘085 design as contrasted against the present design. In essence, Applicants’ design is directed to a security system including a badge, where the badge is not personal to the wearer, but is generic and reusable by various individuals, and is only activated when the individual has been authenticated as belonging to a set of authorized persons. Simply put, in the current design, anyone can use any badge. The de la Huerga ‘085 system is directed to a badge that belongs to or is associated with a specific individual, i.e. is not generic or interchangeable with other similar badges. Everyone must have his or her own personal badge.

The major differences in the two designs can be summarized as follows:

In the present design, a basket of badges could be placed at an access point, such as a front door of a secure facility. None of the badges are identified or associated with any particular individual. An individual could select any badge,

locate herself in front of the administrative computer, including the identity verification system, and be personally verified by the identification verification system, separate from identifying the badge, as belonging to (or not belonging to) a group of authorized individuals. Upon verifying the individual (NOT the badge) with the identity verification system, the administrative computer then loads information, such as access information associated with the individual, onto the generic badge. If the badge somehow becomes disassociated from the individual, any information stored in non-volatile memory in the badge is rendered unreadable. In this manner, Jack cannot switch badges with Mabel and gain access to the computer system posing as Mabel. At the end of the day, the individual can remove her badge, place the badge in the basket, and never have to worry about losing her badge. If the individual mistakenly takes her badge from the secure facility and/or removes the badge from her person, the badge becomes unusable to any other person finding the badge and access to the computer system is unavailable.

See, Specification, p. 17, ll. 13-17:

It should be noted that the badges of the present invention **are not permanently associated with particular individuals**, and hence, an employee does not need to take his or her badge home. **The badges can be picked up from a big basket near station A when needed and thrown back into the basket at the end of the day.** Hence the costs and inconvenience associated with losing or damaging a badge are significantly reduced.

(Emphasis added).

See, also, Specification, Background section, pp. 2-3 (discussing limitations of previous designs: “The authenticity of the card [used in previous designs] can, in principle, be verified by the system that queries the card; however, the system cannot necessarily identify the person presenting the card. An unauthorized person who has gained control of such a card can still access the system.”) (emphasis added). Further, the current Specification describes affixing a badge to a user, such as a clinician, and having the badge “activated” based on personally identifying the clinician, not the

badge: “The affixation of the badge to the user prior to the badge being loaded by terminal 11 can be verified by security personnel stationed at a point that all users must pass before reaching terminal 11....The badge is activated by physically attaching the badge to a clinician and running an authentication protocol between the badge and an administrative computer such as terminal 11 discussed above. During the activation protocol, the administrative computer will verify the clinician’s identity by scanning the clinician’s retina. At the end of the authentication protocol, the badge will be loaded with Cred and thereby activated.” Specification, p. 7, l. 20 – p. 9, l. 10 (emphasis added). Further, in the present design, each badge has a public “username,” denoted by a generic ID. p. 11, l. 27. Thus each badge in the present design is not associated with any particular person.

de la Huerga ‘085, in contrast, provides a badge specifically associated with the individual. See, e.g. FIG. 1, where the badge contains the person’s name and apparently a photo of the person. Information is provided electronically on the badge, such as access privileges and the information shown in, for example, FIG. 8, so that the computer system can determine whether the person possessing the badge has access to the computer system. See, e.g., Col. 9, l. 66 – Col. 10, l. 13; Col. 11, l. 46 – Col. 12, l. 16. The badge is intended to be maintained by one specific person at all times. Notably, the “basket of badges” concept cannot exist using a de la Huerga ‘085 badge, in that each such de la Huerga ‘085 badge is specifically associated with one individual.

Although not explicitly stated in de la Huerga ‘085, information such as access privileges and the other information shown in, for example, FIG. 8, is apparently loaded onto the badge before the badge is provided to the user/employee/wearer. The de la Huerga ‘085 badge is then presumably physically presented to the appropriate individual. (Applicants believe the only statement discussing providing “information” to the de la Huerga ‘085 badge in this regard is at de la Huerga ‘085, Col. 10, ll. 43-44: “An illustration of certain base contents 300 that may be stored by the memory element 262 is set forth in FIG. 8.”)

The de la Huerga '085 badge is thus a typical badge provided by an entity, such as a corporation or the government, to an employee when the employee commences his employment. If the badge is lost, it must be replaced with another personalized badge having the same contents. (See de la Huerga, Col. 13, ll. 5-9: "It is to be expected, however, that should a system user 68 be dispossessed of a security badge 10, that he or she immediately notify the system security administrator to deactivate the access privileges of the security badge.")

The problem with this design is the switching of badges – Mabel could take Jack's badge, either at the facility or elsewhere, and gain access to the computer system posing as Jack. The de la Huerga '085 system verifies the badge, not the individual wearing the badge – a key distinction. Information is not loaded onto the de la Huerga '085 badge in response to or subsequent to verification/authentication of the identity of the person – such personal verification separate from badge verification is not performed, but the badge is simply assumed to belong to the appropriate person. Simply put, the individual takes his de la Huerga '085 badge, places his personal de la Huerga '085 badge in front of the de la Hurega '085 computer system, and is either verified or not verified and granted access to the computer system based on the contents of the badge. This "static personal badge" design thus materially differs from the present design.

Claim 13

Applicant has amended claim 13 to include the following limitations:

determining whether the individual possessing the badge belongs to a set of authorized individuals, said determining comprising evaluating the individual, separate from the badge, using an identity verification system; and

in response to said identity verification system determining the individual belongs to the set of authorized individuals, subsequently causing an administrative device to load information into said volatile memory of said badge, said information specifying the level of access to said computer system to which the individual is entitled.

(Emphasis added).

de la Huerga '085 does not evaluate the individual separate from the badge using an identity verification system.¹ Further, subsequent to, and in response to identifying the individual as belonging to the set of authorized individuals, de la Huerga '085 does not cause an administrative device to load information into said volatile memory of the badge. The static, personal de la Huerga '085 badge already contains the information, such as access privileges, and does not and cannot receive the information enumerated in the claim.

The Office Action cites col 11, l. 46 through col 12, l. 31, as demonstrating how the de la Huerga '085 badge:

intercepts, processes, and returns part of an interrogation signal in a re-crypted form as a return response. This clearly suggests that as part of information exchange, the level of access (consistent with the access privileges) to the network by the security badge is specified. This further suggests 'transmission of information from the administrative computer to the badge'...

Office Action, p. 6. The identified passage, namely the "exchange" between the de la Huerga computer terminal 60 and the de la Huerga badge 10, explains transmission of an interrogation signal from the computer terminal 60 to the badge 10, and in response, the badge 10 "will

¹ de la Huerga '085 does make passing reference to the use of voice identification, fingerprints and retinal scans:

More elaborate means, including voice identification or a fingerprint or retinal scan, could also be incorporated into the security badge 10 or at computer terminals 60 to reinforce such security.

Col. 13, ll. 2-5. First, it is unclear how such means could be incorporated into a badge, and how such a device would work. Second, and more importantly, information personal to the user, such as that shown in FIGs. 1 and 8, would still be located on the de la Huerga '085 badge itself. The badge would remain a static, personal badge with information associated with the user located thereon. Thus the limitations in, for example, claim 13 of "in response to said identity verification system determining the individual belongs to the set of authorized individuals, subsequently causing an administrative device to load information into said volatile memory of said badge" would not be met. In short, the de la Huerga '085 use of voice or fingerprint or retinal information would be in addition to the information already provided on the badge, and no administrative device would "load information" onto the de la Huerga '085 badge, particularly "in response to" voice/fingerprint/retina identification of the individual.

intercept, process, and be operable to return a part of the interrogation signal in re-crypted form.” de la Huerga, Col. 11, ll. 55-57. From the signal sent from the badge 10 to the computer terminal 60, the computer terminal 60 decrypts or authenticates the response using a “private key” which uniquely identifies the system user 68 possessing the key. Col. 12, ll. 3-11. In short, the computer terminal 60 sends an interrogation signal, and the badge 10 sends back part of the interrogation signal and a key identifying the user. Again, no information is loaded onto the badge from the computer terminal, only the signal and key are transmitted from the badge to the computer terminal. Thus the statement that “as part of information exchange, the level of access (consistent with the access privileges) to the network by the security badge is specified” is not applicable. This statement in the Office Action pertains to *the badge 10 providing information to the computer terminal 60*, and not *an administrative device loading information into volatile memory of a badge*, as required by the express language of claim 13. Applicants therefore submit that claim 13, as amended, materially differs from the de la Huerga ‘085 design, and is therefore allowable over the de la Huerga ‘085 reference, either alone or in combination with the de la Huerga ‘086 reference. In short, aspects of claim 13 are missing from both of the cited references. All claims dependent from claim 13 are allowable as containing elements not shown by the cited references.

Claim 17

Claim 17, as amended, now includes the following limitation:

wherein an administrative device may load information in said volatile memory of said badge in response to and subsequent to an identity verification system authenticating an individual maintaining said badge as belonging to a set of authorized individuals, said information specifying the level of access to a client computer to which the individual is entitled.

(Emphasis added).

Again, no administrative device is shown in de la Huerga '085 that loads information in response to and subsequent to an identity verification system authenticating an individual maintaining the badge, where the information loaded in the volatile memory of the badge is the level of access to a client computer to which the individual is entitled. The information provided in de la Huerga '085 from the computer terminal 68 to badge 10 is an interrogation signal, not access level. Further, de la Huerga does not identify/authenticate the person, but just the badge 10.

Thus claim 17, as amended, includes limitations not shown in the cited references. Claim 17 and all claims dependent therefrom are thus allowable over the cited references as containing limitations neither suggested nor disclosed in the references.

Claim 20

Claim 20 recites, *inter alia*:

providing the administrative computer with a transceiver for communicating with the badge and an identity verification system for determining whether the individual, distinct from the badge, belongs to a set of authorized individuals; and

upon determining that the individual possessing the badge personally belongs to the set of authorized individuals, subsequently causing the administrative computer to load information in said volatile memory of said badge, said information specifying the level of access to said computer system to which the individual is entitled.

As with claims 13 and 17, the de la Huerga '085 design does not show such transmission from an administrative computer to a badge. de la Huerga '085 specifically does not cause an administrative computer to load information in volatile memory of a badge upon determining that an individual possessing the badge belongs to a set of authorized individuals, and in particular performing such loading subsequent to determining whether the individual, distinct from a badge, belongs to a set of authorized individuals. de la Huerga '085 instead merely shows transmission of an interrogation signal from a computer terminal 60 to a badge 10, and the badge

providing a part of the interrogation signal and a public key. Thus de la Huerga materially differs from the express language of claim 20. Claim 20 and all claims dependent therefrom are therefore allowable over the cited references.

Accordingly, it is respectfully submitted that all pending claims fully comply with 35 U.S.C. § 103.

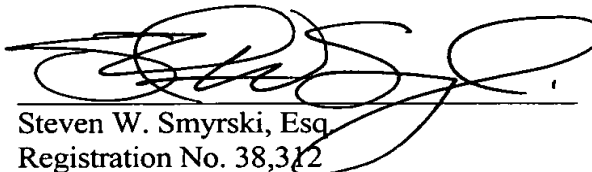
CONCLUSION

In view of the foregoing, it is respectfully submitted that all claims of the present application are in condition for allowance. Reexamination and reconsideration of all of the claims, as amended, are respectfully requested, and allowance of all the claims at an early date is solicited.

Should it be determined for any reason an insufficient fee has been paid, please charge any insufficiency to ensure consideration and allowance of this application to Deposit Account 08-2025.

Respectfully submitted,

Date: June 24, 2004


Steven W. Smyrski, Esq
Registration No. 38,312

SMYRSKI & LIVESAY, LLP
3310 Airport Avenue, SW
Santa Monica, California 90405-6118
Phone: 310.397.9118
Fax: 310.397.9158